IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

In re Search Warrant No. 16-960-M-01 to Google	:	Misc. No.	16-960-M-01
	:		16-1061-M
	:		
In re Search Warrant No. 16-1061-M to Google	:		
	:		

MEMORANDUM OF DECISION

THOMAS J. RUETER
United States Magistrate Judge

February 3, 2017

In August, 2016, this court issued two search warrants, pursuant to section 2703 of the Stored Communications Act, 18 U.S.C. §§ 2701 et seq. ("SCA" or "Act"), which required Google Inc. ("Google") to disclose to agents of the Federal Bureau of Investigation ("FBI") certain electronic data held in the accounts of targets in two separate criminal investigations. Each account holder resides in the United States, the crimes they are suspected of committing occurred solely in the United States, and the electronic data at issue was exchanged between persons located in the United States.

Presently before the court are the Government's motions to compel Google to produce electronic data in accordance with these search warrants (the "Motions").[1] Google has partially complied with the warrants by producing data that is within the scope of the warrants that it could confirm is stored on its servers located in the United States. (N.T. 1/12/17 at 13.) Google, however, has refused to produce other data required to be produced by the warrants, relying upon a recent decision of a panel of the United States Court of Appeals for the Second Circuit, Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by

[1] The Government filed a motion to compel in each of the above-referenced cases. See Case No. 16-960-M-01, Doc. 4 and Case No. 16-1061-M, Doc. 5. The motion filed in each case is essentially the same. Accordingly, the court's analysis applies to both motions.

Microsoft Corp., 829 F.3d 197 (2d Cir. 2016) (hereinafter "Microsoft"), rehearing en banc denied, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017).[2] For the reasons set forth below, the court grants the Motions.

I. BACKGROUND

A. Procedural History

On August 2, 2016, the undersigned issued a search warrant pursuant to section 2703(b) of the SCA, for all data associated with three Google accounts held by an individual who resided in the United States (Case No. 16-960-M-01). The Affidavit in support of the Application for the Search Warrant established probable cause that the three Google accounts described therein were being used by the target of the investigation to commit a fraud in violation of federal law. The fraud described in the Application occurred exclusively in the United States and the victim of the fraud was domiciled in the United States. The executed warrant was served upon Google at its offices in California. The warrant directed Google to send the data to an FBI agent in Pennsylvania.

On August 19, 2016, United States Magistrate Judge M. Faith Angell issued a search warrant (Case No. 16-1061-M) to Google for all data associated with an account of an individual who resided in the United States and was a target of an investigation pertaining to the theft of trade secrets from a corporation located in the United States. The Affidavit in support of

---

[2] On a request for a rehearing en banc, the active judges of the Second Circuit were split evenly (four to four) on whether to grant the petition, and thus the petition was denied. The Honorable Susan L. Carney concurred by opinion in the denial of rehearing en banc. No other judge joined in this opinion. Four judges filed separate opinions dissenting from the denial of rehearing en banc. They were the Honorable Dennis Jacobs, Judge José A. Cabranes, Judge Reena Raggi, and Judge Christopher F. Droney. Each dissenting opinion was joined by the other dissenters.

the Application for the Search Warrant established probable cause that the theft occurred in the United States and this conduct violated federal laws. The warrant was served upon Google at its offices in California. The court allowed "Google to make a digital copy of the entire contents of the information subject to seizure." That copy would be provided to an FBI agent located in Pennsylvania. "The contents [would] then be analyzed to identify records and information subject to seizure." See Aff. ¶ 14(I) filed in support of search warrant.

As explained above, Google did not disclose to the Government all of the user data requested in the two warrants. On October 28, 2016, the Government filed a motion to compel Google to comply with the search warrant, filed at Misc. No. 16-960-M-01 (Doc. 4). On October 28, 2016, this court issued an Order to Google to "show cause in a written response by November 14, 2016 as to the basis upon which Google, Inc. chose not to comply with Search Warrant No. 16-960-M-01 (Doc. 4)." On November 22, 2016, Google filed a Response to November 22, 2016 Order to Show Cause and Motion to Amend Non-Disclosure Order (Doc. 7) ("Google Resp."). In its Response, Google argued that it was not required to produce electronic records stored outside the United States. Google also argued that the warrant is "over broad because it does not describe with particularity which services there is probable cause to search." In addition, Google challenged the non-disclosure order entered by this court pursuant to 18 U.S.C. § 2705(b), contending that the order was an "unconstitutional prior restraint on speech." On January 5, 2017, the Government filed a Reply to Google's Response (Doc. 9) ("Gov't Reply").

The procedural history with respect to the Search Warrant at Misc. No. 16-1061-M is similar. On November 22, 2016, the Government filed a motion to compel Google to

comply with the search warrant (Doc. 5). On November 22, 2016, the court ordered Google to "show cause in a written response to be filed by December 22, 2016 as to the basis upon which Google chose not to comply with Search Warrant No. 16-1061-M." On December 22, 2016, Google, Inc. filed its response to the order to show cause and filed a motion to amend the non-disclosure order (Doc. 7). As in its Response filed in 16-960-M-01, Google relied on the Microsoft case to justify its non-compliance and also challenged the non-disclosure order. On January 5, 2017, the Government filed its reply brief in this case (Doc. 8).

By order dated January 6, 2017, the court granted the parties' joint request for consolidation of the two cases for purpose of the oral argument scheduled on January 12, 2017. The parties submitted a Stipulation of Facts, which was filed in both cases on January 12, 2017.[3] At the hearing, both Google and the Government stressed the importance of the issues raised by the Microsoft case. Google explained that each year it receives thousands of requests for the disclosure of user data from federal, state, and local governmental entities in connection with criminal matters. The Government emphasized the critical importance of obtaining the electronic data of criminal suspects residing in the United States. Due to the priority of the issue to both parties, the court will address the questions arising from the Microsoft decision in this Memorandum of Decision, and will separately decide the over-breath and non-disclosure issues in separate orders.

---

[3] The parties entered into a Stipulation regarding the architecture of Google Inc. and its businesses. See Case No. 16-960-M-01, Doc. 22 and Case No. 16-1061-M, Doc. 11.

B. Stored Communications Act

As noted supra, the search warrants at issue in the present cases were issued under section 2703 of the SCA.[4] The SCA "was born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy arising from illicit access to stored communications in remote computing operations and large data banks that stored e-mails." In re Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 145 (3d Cir. 2015) (internal quotation omitted), cert. denied (2016). Section 2701 of the Act prohibits unauthorized third parties from, inter alia, obtaining, altering or preventing authorized access to an electronic communication stored in a facility through which an electronic communication service is provided. See 18 U.S.C.§ 2701. Section 2701 also imposes criminal penalties for its violation. Id. Subject to certain exceptions, section 2702 of the Act prohibits providers of electronic communication services and remote computing services from disclosing information associated with and contents of stored communications. See 18 U.S.C. § 2702. Significant to the cases at bar, the SCA also empowers the Government to compel a provider to disclose customer information and records. See 18 U.S.C. §§ 2702(b), 2703. The Government may seek information in three ways: by subpoena, court order, or warrant. See 18 U.S.C. § 2703. The particular method chosen by the Government dictates the showing that must be made by the Government and the type of records that must be disclosed in response.

---

[4] The SCA was passed as part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

The Court of Appeals in Microsoft succinctly described the SCA's disclosure structure as follows:

> Regarding governmental access in particular, § 2703 sets up a pyramidal structure governing conditions under which service providers must disclose stored communications to the government. Basic subscriber and transactional information can be obtained simply with an administrative subpoena. 18 U.S.C. § 2703(c)(2). Other non-content records can be obtained by a court order (a "§ 2703(d) order"), which may be issued only upon a statement of "specific and articulable facts showing . . . reasonable grounds to believe that the contents or records . . . are relevant and material to an ongoing criminal investigation." § 2703(c)(2), (d). The government may also obtain some user content with an administrative subpoena or a § 2703(d) order, but only if notice is provided to the service provider's subscriber or customer. § 2703(b)(1)(B).

Microsoft, 829 F.3d at 207. The statutory provisions most relevant to the cases at bar pertain to the court's authority to issue a warrant requiring providers to disclose information and authorizing the Government to search the disclosed information. To obtain such user content, the Act generally requires the government to obtain a warrant that has been issued using the procedures set forth in Rule 41 of the Federal Rules of Criminal Procedure. See 18 U.S.C. § 2703(a)-(c).

C. Federal Rule of Criminal Procedure 41

Rule 41 describes the procedures for the issuance of a search and seizure warrant. Of particular relevance here is Rule 41(b)(5) which provides the following:

> (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within the following:
>
> (A) a United States territory, possession, or commonwealth;
>
> (B) the premises – no matter who owns them – of a United States diplomatic or consular mission in a foreign state, including any

> appurtenant building, part of a building, or land used for the mission's purposes; or
>
> (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41(b)(5).

D. Google's Production of Electronic Data

Google is a United States-headquartered company that provides a variety of online and communications services to its users. (Stip. ¶ 1.) Google stores user data in various locations, some of which are in the United States and some of which are in countries outside the United States. (Stip. ¶ 2.) Some user files may be broken into component parts, and different parts of a single file may be stored in different locations (and, accordingly, different countries) at the same time. (Stip. ¶ 3.) Google operates a state-of-the-art intelligent network that, with respect to some types of data, including some of the data at issue in this case, automatically moves data from one location on Google's network to another as frequently as needed to optimize for performance, reliability, and other efficiencies.[5] (Stip. ¶ 4.) As a result, the country or countries in which specific user data, or components of that data, is located may change. Id. It is possible that the network will change the location of data between the time when the legal process is sought and when it is served. Id. As such, Google contends that it does not currently have the capability, for all of its services, to determine the location of the data and produce that data to a human user at any particular point in time. (N.T. 1/12/17 at 15-16.)

---

[5] Google stores data in a dynamic network which distributes the data, sometimes in bits and pieces, to servers located domestically and in foreign countries. Google maintains data centers across the Americas, Asia and Europe. See www.Google.com/about/datacenters/inside/locations/index.html (last visited February 2, 2017).

At oral argument, counsel for Google explained that each year Google receives over 25,000 pieces of legal process from federal, state, and local governmental entities seeking the disclosure of user data in criminal matters. (N.T. 1/12/17 at 7.) Only Google personnel in Google's Legal Investigations Support team are authorized to access the content of communications in order to produce it in response to legal process. (Stip. ¶ 5.) All such Google personnel are located in the United States. Id. Thus, Google discloses data to the Government by having one of its authorized employees in the United States access the data through its computers located in the United States. Indeed, Google admits that this is the only way data can be accessed in response to legal process and the Government has no other available process to obtain the data.[6] (Stip. ¶ 5; N.T. 1/12/17 at 17.)

Google avers that it has fully complied with the warrants at issue in that it has "produced all records identified with sufficient particularity that are responsive to the warrant(s)." (Google Resp. at 4.) Relying on Microsoft, Google posits that a warrant issued under the SCA "lawfully reaches only data stored within the United States." Id. (citing Microsoft, 829 F.3d at 222). According to Google, it has "already produced all records that it can ascertain are stored within the United States." Id. It further contends that the warrants at issue here cannot compel Google to produce records that are or may be stored outside the United States. Id. To date, therefore, Google has produced only responsive data which it has confirmed to be stored in the United States. See Decl. of John R. Tyler at ¶¶ 1-4. Prior to the Second

---

[6] At oral argument, when asked how the Government could obtain the sought-after data absent Google's production of the data in accordance with the Government's SCA warrant, Google's counsel indicated that the Government could work to reform the SCA. (N.T. 1/12/17 at 17.)

Circuit's decision in Microsoft, Google routinely complied with federal courts' search warrants which commanded the production of user data stored on Google servers located outside the United States. (N.T. 1/12/17 at 8.)

E. The Microsoft Decision

The Microsoft decision was the result of an appeal from an order of the United States District Court for the Southern District of New York which denied Microsoft Corporation's motion to quash a search warrant. In that case, United States Magistrate Judge James C. Francis, IV, issued a search warrant pursuant to the SCA authorizing the search and seizure of information associated with a specific web-based email account maintained by Microsoft Corporation. Microsoft moved to quash the search warrant to the extent it required Microsoft to access user data stored and maintained on servers located in Ireland and import that data into the United States for delivery to federal authorities.

In a comprehensive opinion, Judge Francis denied the motion to quash and held that the warrant did not violate the presumption against extraterritorial application of a law of the United States. In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 15 F.Supp. 3d 466 (S.D.N.Y. 2014). Judge Francis found that under section 2703 of the SCA, the term "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction" is ambiguous regarding jurisdiction. Judge Francis explained as follows:

> This language is ambiguous in at least one critical respect. The words "using the procedures described in the Federal Rules of Criminal Procedure" could be construed to mean, as Microsoft argues, that all aspects of Rule 41 are incorporated by reference in Section 2703(a), including limitations on the territorial reach of a warrant issued under that rule. But, equally plausibly, the

> statutory language could be read to mean that while procedural aspects of the application process are to be drawn from Rule 41 (for example, the presentation of the application based on sworn testimony to a magistrate judge), more substantive rules are derived from other sources. See In re United States, [665 F.Supp. 2d 1210, 1219 (D. Or. 2009)] (finding ambiguity in that "'[i]ssued' may be read to limit the procedures that are applicable under § 2703(a), or it might merely have been used as a shorthand for the process of obtaining, issuing, executing, and returning a warrant, as described in Rule 41"); In re Search of Yahoo, Inc., No. 07-3194, 2007 WL 1539971, at *5 (D. Ariz. May 21, 2007) (finding that "the phrase 'using the procedures described in' the Federal Rules remains ambiguous").

Id. at 470-71. Judge Francis resolved this ambiguity by finding that an SCA warrant is a hybrid between a search warrant and a subpoena. Because an SCA warrant is served on a service provider rather than on a law enforcement officer, it "is executed like a subpoena in that it . . . does not involve government agents entering the premises of the [internet service provider] . . . to search its servers and seize the e-mail account in question." Id. at 471. Thus, the search warrant's subpoena-like qualities required the service provider to hand over information it controls no matter where that information is located. This interpretation was supported by the well-established principle that a court's power to require a person to disclose information applies to all information in that person's custody or control, regardless of where the information is located. See Marc Rich & Co., A.G. v. United States, 707 F.2d 663, 667 (2d Cir. 1983) ("Neither may the witness resist the production of documents on the ground that the documents are located abroad. The test for production of documents is control, not location.").

Judge Francis also held that "it is difficult to believe that, in light of the practical consequences that would follow, Congress intended to limit the reach of the SCA Warrants to data stored in the United States." In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 15 F.Supp. 3d at 474. The court reasoned that allowing

Microsoft to withhold the data stored in Ireland would force the Government to rely solely on Mutual Legal Assistance Treaties ("MLAT"s) to obtain information stored abroad. Judge Francis found that this could not have been Congress' intent as the process under a MLAT is "slow and laborious" and many countries have no MLAT with the United States. Id. at 474-75. Finally, Judge Francis noted that "the concerns that animate the presumption against extra territoriality are simply not present here."

> "[A]n SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored. At least in this instance, it places obligations only on the service provider to act within the United States."

Id. at 475. On July 31, 2014, Chief Judge Loretta A. Preska of the United States District Court for the Southern District of New York affirmed Magistrate Judge Francis' denial of the motion to quash. See In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014). On appeal, the Second Circuit reversed. Microsoft, 829 F.3d 194 (2d Cir. 2016). The majority opinion was authored by the Honorable Susan L. Carney and joined by District Judge Victor A. Bolden. Circuit Judge Gerard E. Lynch filed a concurring opinion.

Significant to the Second Circuit's analytic framework in Microsoft is the principle of construction utilized by the United States Supreme Court in Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247 (2010). The Second Circuit noted the presumption against extraterritorial application of United States statutes analyzed in Morrison to be "strong and binding." Microsoft, 829 F.3d at 209. The court stated:

> When interpreting the laws of the United States, we presume that legislation of Congress "is meant to apply only within the territorial jurisdiction of the United States," unless a contrary intent clearly appears. [Morrison, 561 U.S. at 255] (internal quotation marks omitted); see also RJR Nabisco, Inc. v. European Cmty., 579 U.S. __, __, 136 S. Ct. 2090, 195 L.Ed.2d 476 (2016). This presumption rests on the perception that "Congress ordinarily legislates with respect to domestic, not foreign matters." Id. The presumption reflects that Congress, rather than the courts, has the "facilities necessary" to make policy decisions in the "delicate field of international relations." Kiobel v. Royal Dutch Petroleum Co., __U.S.__, 133 S. Ct. 1659, 1664, 185 L.Ed.2d 671 (2013) (quoting Benz v. Compania Naviera Hidalgo, S.A., 353 U.S. 138, 147, 77 S. Ct. 699, 1 L.Ed.2d 709 (1957)). In line with this recognition, the presumption is applied to protect against "unintended clashes between our laws and those of other nations which could result in international discord." Equal Emp't Opportunity Comm'n v. Arabian American Oil Co., 499 U.S. 244, 248, 111 S. Ct. 1227, 113 L.Ed.2d 274 (1991) ("Aramco"); see generally Parkcentral Global Hub Ltd. v. Porsche Auto. Holdings SE, 763 F.3d 198 (2d Cir. 2014) (per curiam).

Id. at 210. The Second Circuit further explained that, when deciding whether the presumption against extraterritoriality applies to a particular act, a court must evaluate whether language in the relevant act indicates a congressional purpose to extend the coverage of such an act beyond places over which the United States has sovereignty or some measure of legislative control. Id. (citing Aramco, 499 U.S. at 248). "The statutory provision must contain a 'clear indication of an extraterritorial application'; otherwise, 'it has none.'" Id. (citing Morrison, 561 U.S. at 255).

Based on the approach set forth in Morrison, the Second Circuit engaged in a two-part inquiry into the extraterritorial application of the SCA's warrant provisions. The court first analyzed whether the SCA's warrant provisions contemplate extraterritorial application, ultimately concluding that the statute does not indicate that it applies extraterritorially. Id. at 210-11.[7] The court noted that the plain meaning of the SCA supports this finding. Id. at 211. In

---

[7] In Microsoft, the government acknowledged that the warrant provisions of the SCA do not contemplate or permit extraterritorial application. Id. at 210.

addition, the court determined that the term of art "warrant" as used in the SCA was intended to protect privacy rights in a territorial way. Id. at 212.[8]

Having determined under the first step of the Morrison analysis that the relevant statutory provisions of the SCA do not contemplate extraterritorial application, the court proceeded to the second step. That is, the court identified the statute's focus and assessed whether the execution of the warrant would constitute an unlawful extraterritorial application of the SCA. Id. at 220-21. In so doing, the court examined the plain meaning of the SCA's warrant provisions, the focus of the substantive provisions of the Act, the focus of sections 2701 and 2702 of the Act on the protection of stored electronic data, the adoption by the SCA of the procedures set forth in Fed. R. Crim. P. 41 which reflects the historical understanding of a warrant as an instrument protective of a citizen's privacy, and the legislative history of the statute. See id. at 217-20. Ultimately, the Second Circuit found that the SCA focuses on user privacy and determined that enforcing the warrant by directing Microsoft to seize the contents of its customer's communications stored in Ireland would be an unlawful extraterritorial application of the SCA. Id. at 220-21.

F. Morrison Step Two Analysis

In a recent decision, the Supreme Court further elaborated on the proper analysis at step two of the Morrison inquiry. In RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090

---

[8] The court rejected the district court's interpretation of the word "warrant" as used in 18 U.S.C. § 2703(a) as one being akin to a hybrid between a warrant and a subpoena. Microsoft, 829 F.3d at 213-14. Instead, the Second Circuit held that the term warrant was a term of art, tied to the restrictions of Fed. R. Crim. P. 41(b)(5) which limits search warrants to a United States territory, possession or commonwealth. The court noted that the SCA itself distinguishes between subpoenas and warrants and the Act does not use the word "hybrid" to describe a warrant. See id. at 214-16.

(2016), the Court considered the extraterritorial application of two separate sections of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961 et seq. ("RICO"), and applied the principles of Morrison to its analysis. In RJR Nabisco, the Court considered whether RICO's substantive prohibitions, contained in § 1962, apply to conduct that occurs in foreign countries and whether RICO's private right of action, contained in § 1964(c), applies to injuries that are suffered in foreign countries. In its analysis, the Court reiterated that the first step of the Morrison framework asks "whether the presumption against extraterritoriality has been rebutted – that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially." Id. at 2101. When describing the second step of the Morrison analysis, the Court again indicated that it requires the reviewing court to look at the statute's "focus" to determine whether the case involves a domestic application of the statute. Id. The Court further elaborated, stating:

> If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory.

Id. Given the facts of the case before it, and in light of the statutory provisions at issue, the Court did not employ the second step of the Morrison analysis as it described. Ultimately, the Court determined that the substantive prohibitions of § 1962 of RICO may apply to foreign conduct and concluded that the presumption against extraterritoriality was rebutted but only with respect to certain applications of the statute. Id. at 2101-06. The Court also held that § 1964(c) requires a

civil RICO plaintiff to allege and prove a domestic injury to business or property and does not allow recovery for foreign injuries. Id. at 2111.[9]

II. DISCUSSION

Much like the issues presented in Microsoft, the present dispute centers on the nature and reach of the warrants issued pursuant to the SCA. The court must determine whether the Government may compel Google to produce electronic records relating to user accounts pursuant to search warrants issued under section 2703 of the SCA, or in the alternative, whether Google has provided all records in its possession that the Government may lawfully compel Google to produce in accordance with the Second Circuit's ruling in Microsoft. The Government urges this court to depart from the Second Circuit's reasoning in Microsoft and compel disclosure by Google of the relevant electronic data. See Gov't Reply at 3-25. The Government argues that the Microsoft decision is incorrect, inconsistent with the weight of authority, not binding on this court, and should not be followed. For the reasons that follow, this court concludes that compelling Google to disclose to the Government the data that is the subject of the warrants does not constitute an unlawful extraterritorial application of the Act.

---

[9] Since the RJR Nabisco case was decided, other courts have applied the RJR Nabisco interpretation of the Morrison second step. See, e.g., Adhikari v. Kellogg Brown & Root, Inc., 845 F.3d 184, 194-96 (5th Cir. 2017) (following guidance of RJR Nabisco and analyzing whether there was any domestic conduct relevant to the plaintiffs' claims under the Alien Tort Statute); see also Tatung Co., Ltd. v. Shu Tze Hsu, 2016 WL 6683201, at *8 (C.D. Cal. Nov. 14, 2016) (analyzing whether the plaintiff suffered a domestic injury to business or property for the purposes of civil RICO's private right of action); Bascuñan v. Daniel Yarur ELS Amended ComplaintA, 2016 WL 5475998, at *6 (S.D.N.Y. Sept. 28, 2016) (to determine whether a plaintiff may maintain a private cause of action under § 1964(c), the court must consider where the alleged injury was suffered).

A. Application of the Morrison Analysis

As an initial matter, the court notes that the parties do not dispute the Second Circuit's conclusion at the first step of the Morrison framework – that Congress did not intend the SCA's warrant provisions to apply extraterritorially. Rather, the Government takes issue with the second step of the Morrison analysis as applied by the Second Circuit in Microsoft. The Government argues that the Second Circuit erred when it determined that the "focus" of section 2703 of the SCA is privacy, as opposed to disclosure.[10] However, the court will assume, arguendo, that the focus of the SCA's warrant provisions is privacy as the Second Circuit reasoned.

With this "focus" in mind, a reviewing court must determine whether the case involves a domestic application of the SCA. See RJR Nabisco, 136 S. Ct. at 2101. To do so, the court must examine where the conduct relevant to the statute's focus occurred. See id. ("If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory.").

1. Analysis of Extraterritoriality in Microsoft

With respect to this portion of the Morrison framework, the Microsoft court examined where the electronic data was "seized" and the "invasion of the customer's privacy

---

[10] Relying on Morrison and RJR Nabisco, the Government contends that step two of a proper extraterritoriality analysis should proceed on a section by section basis. See Gov't Reply at 13-16. According to the Government, the Second Circuit incorrectly concluded that privacy concerns trump the actual focus of § 2703, which is disclosure.

takes place." 829 F.3d at 220.[11] The Second Circuit found that the SCA warrant had extraterritorial application because "the content to be seized is stored in Dublin [Ireland]." Id. The court explained:

> Although the Act's focus on the customer's privacy might suggest that the customer's actual location or citizenship would be important to the extraterritoriality analysis, it is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed – here, where it is seized by Microsoft, acting as an agent of the government. Because the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States.

Id. at 220-21. The court ultimately concluded that enforcement of the warrant, insofar as it directs Microsoft to seize the contents of its customer's communications stored in Ireland,

---

[11] The Second Circuit used familiar Fourth Amendment terms such as "seizure" and "invasion of privacy" to determine whether the search warrant was applied extraterritorially. See Microsoft, 829 F.3d at 220. The court described the SCA's privacy protections as "analogous" to those guaranteed by the Fourth Amendment. Id. at 206 (The SCA's legislative history shows Congress' intent "to extend to electronic records privacy protections analogous to those provided by the Fourth Amendment."). Moreover, the court rejected the district court's conclusion that the search warrant was a hybrid between a subpoena and a search warrant, but found it to be a traditional search warrant, which carried with it the territorial restrictions of Fed. R. Crim. P. 41(b)(5). See id. at 214-15 ("We see no reason to believe that Congress intended to jettison the centuries of law requiring the issuance and performance of warrants in specified, domestic locations, or to replace the traditional warrant with a novel instrument of international application."). The court thus found that because a warrant procured under section 2703 of the SCA is a traditional warrant, it is appropriate to analyze the application of the search and seizure warrant under the Fourth Amendment's "seizure" and "invasion of privacy" principles. See id. at 212 ("[A] warrant is traditionally moored to privacy concepts. . . ."). This court notes that the Fourth Amendment provides even greater privacy protection than the SCA. See United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2011) (Fourth Amendment rights of a person were violated by compelling internet service provider to turn over emails without first obtaining a warrant based on probable cause even though sections 2703(b) and 2703(d) of the SCA permitted the disclosure).

constitutes an unlawful extraterritorial application of the Act.[12]

2. Analysis of Extraterritoriality in the Present Cases

In contrast to the decision in Microsoft, this court holds that the disclosure by Google of the electronic data relevant to the warrants at issue here constitutes neither a "seizure" nor a "search" of the targets' data in a foreign country. This court agrees with the Second Circuit's reliance upon Fourth Amendment principles, but respectfully disagrees with the Second Circuit's analysis regarding the location of the seizure and the invasion of privacy. The crux of the issue before the court is as follows: assuming the focus of the Act is on privacy concerns, where do the invasions of privacy take place? To make that determination, the court must

---

[12] As noted supra, the Honorable Gerard E. Lynch filed a concurring opinion in the Microsoft panel decision. See Microsoft, 829 F.3d at 222-33. Judge Lynch found that because of the amorphous nature of cloud technology, the question of whether compelling disclosure of data stored in Ireland constituted an extraterritorial application of the SCA was a "very close" question. He stated, "[t]he government's characterization of the warrant at issue as domestic, rather than extraterritorial, is thus far from frivolous and renders this, for me, a very close case to the extent that the presumption against extraterritoriality shapes our interpretation of the statute." Id. at 229. Judge Lynch explained:

> Corporate employees in the United States can review . . . [electronic documents], when responding to the "warrant" or subpoena or court order just as they can do in the ordinary course of business, and provide the relevant materials to the demanding government agency, without ever leaving their desks in the United States. The entire process of compliance takes place domestically.

Id. at 229. Judge Lynch criticized the majority's finding that "the locus of the invasion of privacy is where the private content is stored." Id. at 230 n.7. He stated that this determination seemed to be "suspect when the content consists of emails stored in the 'cloud.'" Id. He stated, "[i]t seems at least equally persuasive that the invasion of privacy occurs where the person whose privacy is invaded customarily resides." Id. However, Judge Lynch ultimately concluded that because the nationality of the Microsoft account holder was unknown and was probably a citizen of Ireland, Congress did not intend for the SCA "to reach situations of this kind." Id. at 230. He explained that the case would be different "if the American government is demanding from an American company e-mails of an American citizen resident in the United States, which are accessible at the push of a button in Redmond, Washington." Id.

analyze where the seizures, if any, occur and where the searches of user data take place. This requires the court to examine relevant Fourth Amendment precedent. The court recognizes that the cases discussed below address seizures and searches of physical property. However, these cases are instructive, and binding, in the absence of Supreme Court or Third Circuit caselaw addressing such issues as they pertain to the electronic world.

The Fourth Amendment "protects two types of expectations, one involving 'searches' the other 'seizures.'" United States v. Jacobsen, 466 U.S. 109, 113 (1984). The Amendment "protects property as well as privacy." Soldal v. Cook Cty., Ill., 506 U.S. 56, 62 (1992). "A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed." Jacobsen, 466 U.S. at 113. "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." Id. See also United States v. Jones, 132 S. Ct. 945, 958 (2012) (Alito, J., concurring) (same); California v. Hodari D., 499 U.S. 621, 624 (1991) ("From the time of the founding to the present, the word 'seizure' has meant a 'taking possession.'"); Mark Taticchi, Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures, 78 Geo. Wash. L. Rev. 476, 477 (2010) ("Courts generally interpret possessory interest to mean physical possession, even when the property allegedly seized is intangible, like information.").[13]

---

[13] The Supreme Court has stated with respect to the distinction between a "seizure" and a "search":

> Although our Fourth Amendment cases sometimes refer indiscriminately to searches and seizures, there are important differences between the two . . . . The Amendment protects two different interests of the citizen – the interest in retaining possession of property and the interest in maintaining personal privacy. A seizure threatens the former, a search the latter. As a matter of timing, a seizure is usually preceded by a search, but when a container is involved the converse is

Electronically transferring data from a server in a foreign country to Google's data center in California does not amount to a "seizure" because there is no meaningful interference with the account holder's possessory interest in the user data. Indeed, according to the Stipulation entered into by Google and the Government, Google regularly transfers user data from one data center to another without the customer's knowledge. Such transfers do not interfere with the customer's access or possessory interest in the user data. Even if the transfer interferes with the account owner's control over his information, this interference is de minimis and temporary. See Jacobsen, 466 U.S. at 125-26 (holding that permanent destruction of small portion of property for testing a de minimis intrusion on possessory interest); United States v. Hoang, 486 F.3d 1156, 1162 (9th Cir. 2007) ("[N]o seizure occurs if a package is detained in a manner that does not significantly interfere with its timely delivery in the normal course of business."), cert. denied, 552 U.S. 1144 (2008).

This conclusion is supported by the Supreme Court's decision in Arizona v. Hicks, 480 U.S. 321 (1987). In Hicks, a police officer was searching an apartment under exigent circumstances when he noticed an expensive stereo system that he suspected had been stolen. Id. at 323. Accordingly, he wrote down the serial number of some of its components. He later confirmed that the serial numbers matched stereo components stolen during an armed robbery.

> often true. Significantly, the two protected interests are not always present to the same extent; for example, the seizure of a locked suitcase does not necessarily compromise the secrecy of its contents, and the search of a stopped vehicle does not necessarily deprive its owner of possession.

Texas v. Brown, 460 U.S. 730, 747-48 (1983) (Stevens, J., concurring).

Id. at 323-24. The Supreme Court found that copying the serial numbers did not constitute a "seizure" under the Fourth Amendment. The Court explained:

> We agree that the mere recording of the serial numbers did not constitute a seizure. To be sure, that was the first step in a process by which respondent was eventually deprived of the stereo equipment. In and of itself, however, it did not "meaningfully interfere" with respondent's possessory interest in either the serial numbers or the equipment, and therefore did not amount to a seizure.

Id. at 324. Following Hicks, the Third Circuit has held that a police officer's movement of documents from one place to another so that the documents could be reviewed by another law enforcement officer did not constitute a seizure. United States v. Menon, 24 F.3d 550, 559-60 (3d Cir. 1994) (Becker, J). The court reasoned that the police officer did not seize the documents at issue when she carried the documents from one office to an adjacent office because such movement did not meaningfully interfere with the possessory interest of the individual from whose office the documents were taken. Id. at 560.

Other circuit courts have held that photocopying documents or taking photographs of materials did not constitute a "seizure" because such actions did not meaningfully interfere with the owners' possessory interest. See United States v. Mancari, 463 F.3d 590, 596 (7th Cir. 2006) (photographs); Bills v. Aseltine, 958 F.2d 697, 707 (6th Cir. 1992) (photographs); United States v. Thomas, 613 F.2d 787, 794 (10th Cir. 1980) (photocopies). It is not surprising, therefore, that two district courts have held that accessing electronic data is not a "seizure." See In re United States, 665 F.Supp. 2d 1210, 1222 (D. Or. 2009) (court found no "seizure" because there was no "meaningful interference due to the nature of electronic information, which can be accessed from multiple locations, by multiple people, simultaneously."); United States v. Gorshkov, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001) (FBI agent's act of copying

data on computer was not a "seizure" under the Fourth Amendment because it did not interfere with the defendant's possessory interest in the data).[14] For these reasons, the execution of the two Google search warrants, at issue here, will not result in a "seizure" in a foreign country.[15]

The court's Fourth Amendment analysis does not end there, however, for the court also must examine the location of the searches in the instant cases. As noted supra,

---

[14] Rule 41(e)(2)(B), which deals with a warrant seeking electronically stored information, provides:

> A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Fed. R. Crim. P. 41(e)(2)(B). One commentator posits that the express language of Rule 41 reinforces the view that copying information does not constitute a seizure. See Taticchi, supra, at 489. By joining "copying" and "seizure" with the conjunction "or" the rule implies "that the two concepts do not overlap, i.e., that copying is not a seizure." Id. Rule 41(f) also refers to seizures and copies as alternative options. Id.

[15] This court's conclusion that a "seizure" would not occur when Google accesses the undisclosed electronic data required by the two warrants also is supported by Judge Raggi's dissenting opinion from the denial of rehearing en banc. This opinion was joined by the three other dissenting judges of the Second Circuit. Judge Raggi found:

> even if privacy is the focus of §§ 2702 and 2703, the territorial event that is the focus of that privacy interest is the service provider's disclosure of the subscriber communications to a third party – whether in violation of § 2702(a) or as authorized by warrant under § 2703(a). It is where that disclosure occurs that determines whether these statutory provisions are being applied domestically or extraterritorially.

2017 WL 362765, at *16. Judge Raggi also rejected the majority panel's ruling that Microsoft's accessing of the emails in Ireland constituted a "seizure." Judge Raggi reasoned that "it is simply wrong to characterize Microsoft's actions in retrieving customer electronic data in Ireland as "'Microsoft's execution of the warrant,'" much less as a seizure by Microsoft." Id. at *15 (citing Carney, J., Op. at 3; Microsoft, 829 F.3d at 220).

pursuant to Fourth Amendment precedent, a "search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001) (citing Katz v. United States, 389 U.S. 347, 361 (1967)). When Google produces the electronic data in accordance with the search warrants and the Government views it, the actual invasion of the account holders' privacy – the searches – will occur in the United States. Even though the retrieval of the electronic data by Google from its multiple data centers abroad has the potential for an invasion of privacy, the actual infringement of privacy occurs at the time of disclosure in the United States. See United States v. Karo, 468 U.S. 705, 712 (1984) ("[W]e have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment. A holding to that effect would mean that a policeman walking down the street carrying a parabolic microphone capable of picking up conversations in nearby homes would be engaging in a search even if the microphone were not turned on."). See also Jones, 132 S. Ct. at 958 ("It is clear that the attachment of the GPS device was not itself a search; if the device had not functioned or if the officers had not used it, no information would have been obtained.") (Alito, J. concurring).[16]

---

[16] Federal Rule of Criminal Procedure 41(e)(2)(B) allows law enforcement officers to copy the electronic data and review it at a later time to determine what electronic stored data falls within the scope of the warrant. See also Orin S. Kerr, Fourth Amendment Seizures of Computer Data, 119 Yale L.J. 700, 711 (2010) ("When the government makes an electronic copy of data, it obtains possession of the data that it can preserve for future use. To be sure, subsequently viewing the data in the copy and thus exposing its contents ordinarily amounts to a Fourth Amendment search."); Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 551 (2005) ("[A] search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer.").

Under the facts before this court, the conduct relevant to the SCA's focus will occur in the United States. That is, the invasions of privacy will occur in the United States; the searches of the electronic data disclosed by Google pursuant to the warrants will occur in the United States when the FBI reviews the copies of the requested data in Pennsylvania. These cases, therefore, involve a permissible domestic application of the SCA, even if other conduct (the electronic transfer of data) occurs abroad. See RJR Nabisco, 136 S. Ct. at 2101.[17]

B. Other Considerations

Having concluded that the record before the court does not present an extraterritorial application of the SCA, the court will address several other considerations raised by the parties, recognizing that such considerations are not determinative of the primary issue before the court. In this court's view, the analysis set forth above does not run afoul of principles of comity and also presents a commonsense interpretation of the SCA which will not lead to absurd results.

---

[17] In contrast to the facts in Microsoft, there is no evidence in our record regarding the precise location of the servers which store the electronic data requested by the search warrants. Therefore, Google's case is easily distinguishable from the facts in Microsoft, wherein all the relevant user data of a presumably Irish citizen was located exclusively in one data center in Ireland and remained stable there for a significant period of time. See Microsoft, 829 F.3d at 220 (finding "that the data is stored [exclusively] in Dublin, that Microsoft will necessarily interact with the Dublin data center in order to retrieve the information for the government's benefit, and that the data is within the jurisdiction of a foreign sovereign"). Indeed, a key assumption made by the majority in Microsoft was that "messages stored in the 'cloud' have a discernable physical location." Id. at 221 n.28. As explained supra, because of the changeable and divisible nature of Google's cloud technology, this critical assumption cannot be made in this case. See Jennifer Daskal, The Un-Territoriality of Data, 125 Yale L.J. 326, 379 (2015) ("The intermingling of data means that it is often difficult, if not impossible, to make the kind of fine-tuned identity – and location – based distinctions that Fourth Amendment . . . law demands.").

1. Risks to International Comity

The court acknowledges that the presumption against extraterritorial application is utilized to protect against "unintended clashes between our laws and those of other nations which could result in international discord." Microsoft, 829 F.3d at 210 (quoting Equal Emp't Opportunity Comm'n v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991)). One scholar has suggested that when determining whether a search and seizure warrant for electronic data has been applied extraterritorially, the court should not look to where the Fourth Amendment seizure or invasion of privacy occurred, as the Second Circuit majority panel did in Microsoft, but whether there was interference with a foreign state's sovereignty to determine its own rules regarding privacy of data stored in its domestic server. See Daskal, supra at 372 n.170. However, Judge Cabranes, in his opinion dissenting from the denial of rehearing en banc, stated that "Morrison . . . does not permit a court to conclude that a particular application of a statute is extraterritorial simply because it believes that the application threatens international comity." See 2017 WL 362765, at *9 n.23 (Cabranes, J., dissenting).

Even if the interference with a foreign state's sovereignty is implicated, the fluid nature of Google's cloud technology makes it uncertain which foreign country's sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process. As explained earlier, Google's architecture not only divides user data among data centers located in different countries, but also partitions user data into shards. Furthermore, the data automatically moves data from one location on Google's network to another as frequently as needed, to optimize for performance, reliability and other efficiencies.

See Stip. ¶ 4; N.T. 1/12/17 at 16.[18] Because of the structure of this system, Google cannot say with any certainty which foreign country's sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process. Before a court bars the Government from using a judicially approved search warrant to require disclosure of user data that constitute evidence of crimes, it would do well not to be controlled by possibilities and legal abstractions, but to focus instead on realities.

Furthermore, it bears repeating that under the facts presented to this court, the searches pursuant to the SCA warrants will occur in Pennsylvania. No foreign nation's sovereignty will be interfered with in any ascertainable way at the time the two warrants at issue are executed because the searches will be conducted in the United States.

2. Reasonable Interpretation

In addition to the presumption against extraterritorial application, a court interpreting the SCA should consider another important canon of construction. Specifically, courts should avoid an interpretation of a statute that produces odd or absurd results, or that is inconsistent with common sense. See Disabled in Action of Pa. v. Southeastern Pa. Trans. Auth., 539 F.3d 199, 210 (3d Cir. 2008) (citations omitted). "Statutes should be interpreted to avoid untenable distinctions and unreasonable results whenever possible." Am. Tobacco v. Patterson, 456 U.S. 63, 71 (1982). See also Register v. PNC Fin. Serv. Grp., Inc., 477 F.3d 56, 67 (3d Cir. 2009) (same). To interpret the SCA as propounded by the majority panel in Microsoft, would lead to an unreasonable result in the cases at bar.

---

[18] "[W]hen one stores data in the cloud, one often has little control or even knowledge about the places where it is being held; these are decisions that are instead generally entrusted to computer algorithms." Daskal, supra at 368.

In Microsoft, the Government alleged that preventing SCA warrants from reaching data stored abroad would place a substantial burden on the Government; the Government further argued that the current process for obtaining foreign-stored data is cumbersome. Microsoft, 829 F.3d at 221. That process is governed by a series of MLATs between the United States and other countries, pursuant to which signatory states may request one another's assistance with ongoing criminal investigations, including the power to summon witnesses, to compel the production of documents and other real evidence, to issue search warrants, and to serve process. See U.S. Dep't of State, 7 Foreign Affairs Manual (FAM) § 962.1 (2013), https://fam.state.gov/FAM/07FAM/07FAM0960.html. But as the district court in Microsoft found, the process under an MLAT is "slow and laborious" and many countries have no MLAT with the United States. Microsoft, 15 F.Supp. 3d at 474-75. This concern was echoed by Judge Cabranes in his opinion dissenting from the denial of en banc review of the Microsoft decision. Judge Cabranes stated:

> The United States has entered into MLATs with several countries, allowing parties to the treaty to request assistance with ongoing criminal investigations, including issuance and execution of search warrants. However, many countries do not have MLATs with the United States, e.g., Indonesia and Pakistan, and law enforcement cooperation with those countries is limited.

2017 WL 362765, at *8 n.11.

In addition, the Government argues that Google's architecture creates an insurmountable obstacle for the Government to overcome in the MLAT process. The location of the electronic data depends "upon the working of an automatic computer algorithm aimed at creating network efficiency." See Gov't Reply at 20. The Government seeks to draw a distinction between Microsoft and the present case. In Microsoft, the ISP could inform the

Government that the data was located in Ireland and that it would remain in Ireland while the Government sought process, either under an MLAT request, or by using Letters Rogatory. In the present case, however, the Government never will be able to utilize established legal process to request assistance from a foreign nation to access Google's user data that is stored in that foreign nation. Google admits that the location of the data could change from the time the Government applies for legal process to the time when the process is served upon Google. See Stip. ¶ 4. The Government explained the problem:

> The data, however, is a moving target: stored one day in a data center in Finland or Singapore; and automatically moved the next day to a new data center in Chile, or Belgium. Further complicating things is that Google user data - such as an e-mail, or an e-mail attachment - is not stored as one single, cohesive digital file; instead, Google stores individual data files in multiple data "shards," each separate shard being stored in separate locations around the world. And, Google cannot even determine where its separate data shards are stored around the world at any given time; and, even if one shard were to stay in one place, without *all* of the shards being collected and put together at once to form the actual digital file, each shard alone is a useless piece of coded gibberish. Of course, each shard might move instantaneously to somewhere else; and then to somewhere else; and so on, and so forth.
>
> . . . .
>
> Thus Google has created a system in which Google can retrieve the data, and its users can retrieve the data, but the government will only be able to obtain data that happens to be stored in the United States at the very moment when Google gathers the responsive information. Google cannot say where its foreign-stored data is today, and to the extent that it can, such data may be automatically moved to another server in another country within short periods. The government, therefore, cannot request the assistance of a foreign country using an MLAT request or Letters Rogatory, because no one knows which country to ask, and even if specific servers could be identified, the data may no longer be there by the time its location has been identified. Moreover, there are no Google employees in other countries that can access their foreign-stored data; instead, such data must, as a consequence of their network architecture, be accessed from a Google employee within the United States. And, thus, certain Google user data - even data that the government knows about, and writes about within a search warrant affidavit - is never accessible through compulsory legal process. Never.

(Gov't Reply at 21-22) (footnote omitted) (emphasis in original). Thus, if the court were to adopt Google's interpretation of the Microsoft decision and apply such a rationale to the case at bar, it would be impossible for the Government to obtain the sought-after user data through existing MLAT channels. In contrast, under this court's interpretation, Google will gather the requested undisclosed data on its computers in California, copy the data in California, and send the data to law enforcement agents in the United States, who will then conduct their searches in the United States.

After careful consideration of the views of the parties and the many eminent judges who have addressed issues arising under the SCA, this court concludes that the two search warrants executed upon Google in the cases at bar do not constitute extraterritorial applications of the SCA.

II. CONCLUSION

For all the above reasons, the court will grant the Government's motions to compel Google to comply with search warrants. An appropriate order follows.

BY THE COURT:

Thomas J. Rueter

THOMAS J. RUETER
United States Magistrate Judge